REMARKS

The above amendments to the above-captioned application along with the following remarks are being submitted as a full and complete response to the Office Action dated March 29, 2006 (U.S. Patent Office Paper No. 20060214). In view of the above amendments and the following remarks, the Examiner is respectfully requested to give due reconsideration to this application, to indicate the allowability of the claims, and to pass this case to issue.

Examiner Interview

On June 27, 2006, Applicants' representative conducted a telephone interview with the Examiner, presenting proposed amendments and discussing the prior art of record. Applicants' representative discussed with the Examiner that a distinctive feature of the present invention is the conversion of the original optimization problem in a client computer system, the solving of the converted optimization problem in a server with a method for solving a linear programming method, and then the reconverting of the solution for the converted optimization problem in the client computer system. The Examiner disagreed alleging that the reference of Matsumoto (as noted hereinbelow) shows similar features. No agreement was reached during the interview. Applicants respectfully thank the Examiner for his consideration in conducting an interview with Applicants' representative.

Status of the Claims

As outlined above, claim 9 stands for consideration in this application, wherein claim 9 is being amended to correct formal errors and to more particularly point out and distinctly claim the subject invention. Claims 2 - 4 stand withdrawn from consideration in this application.

Additional Amendments

The specification is being amended to correct formal errors and to better disclose and describe the features of the present invention as claimed.

All amendments to the application are fully supported therein, including page 17, line 8 - page, 20, line 13 of the specification. Applicant hereby submits that no new matter is being introduced into the application through the submission of this response.

Formal Objections

Claim 9 was objected to for informalities on the grounds that the phrase "with using a ciphering key" is awkward. Claim 9 is being amended so as to delete the limitation which includes the phase "with using a ciphering key." Accordingly, withdrawal of this objection is respectfully requested.

Prior Art Rejections

35 U.S.C. §103(a) rejection

Claim 9 was rejected under 35 U.S.C. §103(a) as being allegedly unpatentable over Matsumoto et al. ("Speeding up Secret Computations with insecure Auxiliary Devices," Advances in Cryptology-Crypto' 88, Springer-Verlag Berlin Heidelberg. 1990. pp. 497-506) in view of England (US Pat. No. 6,996,236). This rejection is respectfully traversed for the reasons set forth below.

According to the Manual of Patent Examining Procedure (M.P.E.P. §2143),

> To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both not found in the prior art, not in the applicant's disclosure.

The Office Action contends that Matsumoto discloses all the limitations recited in claim 9 except generating P and Q using a ciphering key, although Matsumoto discloses that P and Q are randomly generated. The Office Action further contends that England discloses the well-known idea that a ciphering key may drive a random generator, and that it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the ideas of England with those of Matsumoto and using a ciphering key in the random generation process on the ground doing so is an effective means to create random values. Applicants respectfully disagree.

The present invention is directed to a system in which upon a request to solve an optimization problem, information of the problem, the solution and ciphering key is not delivered on a network. (page 6, lines 9-15 of the specification)

The distinctive features, among others, of the present invention as now recited in claim 9 are (1) generating nonsingular matrix P, namely, (2) generating a left permutation matrix P_1 having m rows and m columns and a right permutation matrix Q_1 having n rows and m columns for transforming the coefficient matrix A of the original problems into a bordered block diagonal form; (3) choosing one row of a matrix P_1AQ_1 by using a first random number, choosing another row of the matrix P_1AQ_1 which belongs to the same diagonal block as the chosen row by using a second random number where the first chosen row is referred to as L_1th row and the second chosen row is referred to as L_2th row, adding a third random number r to a (L_1,L_2) th component of a unit matrix having m rows and m columns, and adding a fourth random number s to a (L_2, L_1)th component of the unit matrix thereby to generate a matrix P_1; (4) choosing one column of the matrix P_1AQ_1 by using a fifth random number and choosing another column of the matrix P_1AQ_1 which belongs to the same diagonal block as the chosen column is chosen by using a sixth random number, where the first chosen row is referred to as R_1th row and the second chosen row is referred to as R_2th row, thereby to generate a matrix Q_1'; and (5) generating P_2', Q_2', P_3', Q_3', ..., P_n', Q_n' by sequentially using random numbers included in the ciphering key, generating a matrix P2 and a matrix Q2 according to the relations $P_2 = P_n' \ldots P_2' P_1'$ and $Q_2 = Q_1, Q_2' \ldots Q_n'$, and generating the nonsingular matrix P having m rows and m columns and the permutation matrix Q having n rows and n columns by using the relations $P = P_2P_1$ and $Q = Q_1Q_2$.

In contrast, Matsumoto merely shows a general description of a method to solve a linear equation $AX = B$ by generating permutation matrices, where X is a solution to be obtained, A is a secret non-singular matrix and a secret matrix. However, Matsumoto says nothing about the details of generating permutation matrices with a ciphering key, as now recited in claim 9.

England is directed to a method for protecting copyrighted information such as video signals from unauthorized use. England shows that the source and destination device include a psuedo-random number generator driven by a session key which is used for encrypting the analog signals. England, however, says nothing about the elements that Matsumoto fails to show or suggest.

Furthermore, there is no suggestion or motivation in either Matsumoto or England to combine these features explicitly or implicitly, or in the knowledge generally available to one of ordinary skill in the art at the time the invention was made to embody all the features of

the invention as recited in claim 9. Accordingly, claim 9 is not obvious in view of all the prior art.

Conclusion

In view of all the above, Applicants respectfully submit that certain clear and distinct differences as discussed exist between the present invention as now claimed and the prior art references upon which the rejections in the Office Action rely. These differences are more than sufficient that the present invention as now claimed would not have been anticipated nor rendered obvious given the prior art. Rather, the present invention as a whole is distinguishable, and thereby allowable over the prior art.

Favorable reconsideration of this application as amended is respectfully solicited. Should there be any outstanding issues requiring discussion that would further the prosecution and allowance of the above-captioned application, the Examiner is invited to contact the Applicant's undersigned representative at the address and phone number indicated below.

Respectfully submitted,

Stanley P. Fisher
Registration Number 24,344

Juan Carlos A. Marquez
Registration Number 34,072

REED SMITH LLP
3110 Fairview Park Drive
Suite 1400
Falls Church, Virginia 22042
(703) 641-4200

July 27, 2006